T La gestión en redes definidas por software (SDN) desde la perspectiva de FCAPS

José Roberto Santamaría Sandoval

1. Universidad Estatal a Distancia, Vicerrectoría Académica, Escuelas de Ciencias Exactas y Naturales, Licenciatura en Ingeniería en Telecomunicaciones, 2050 Sabanilla, San José, Costa Rica; jsantamarias@uned.ac.cr

Recibido: 13 de abril de 2020 Aceptado: 08 de setiembre de 2020

RESUMEN

Una nueva arquitectura de comunicaciones establece nuevos retos, en el caso de SDN en términos de la gestión. Este trabajo analiza la gestión en redes SDN desde la perspectiva de FCAPS. La metodología de investigación es revisión bibliográfica de distintas fuentes de información como artículos científicos, documentos de proveedores y normativas para realizar una descripción sobre la arquitectura SDN, modelo FCAPS y la aplicación de FCAPS sobre SDN. Los resultados más importantes son la comprensión de la gestión en SDN y su protocolo OpenFlow, así como sus diferencias con el modelo tradicional de gestión. El segundo resultado importante es la necesidad del desarrollo de complementos a OpenFlow para dar cabalidad a todas las funciones definidas en un modelo FCAPS. Del trabajo sé concluye que la gestión de SDN si es posible visualizarla desde la perspectiva FCAPS, pero tiene una serie de brechas que son cubiertas con desarrollos complementarios. Aun así, se visualiza que SDN podrá cubrir todas las funcionalidades de FCAPS en el corto plazo por el tiempo reciente que tiene esta arquitectura en términos tecnológicos.

Palabras claves: Arquitectura, comunicaciones, modelo, gestión, protocolos, SDN

ABSTRACT

The development of a new communication architecture establishes new challenges, in the case of SDN in terms of management. The study analyzes SDN networks management from the FCAPS perspective. The investigation methodology includes review of different sources of information such as scientific articles, supplier documents and regulations to make a description about SDN architecture, FCAPS model and FCPAS application on SDN. Among the main results are understanding management in SDN and its management protocol called OpenFlow and its differences with the traditional model and SNMP. Second, OpenFlow needs the plugins development to fully support all FCAPS functions. The main conclusions are SDN management is possible to be analyze and evaluate from the FCAPS perspective. Second, SDN management has gaps versus FCAPS model that are covered with complementary developments. Third, SDN can achieve all the functionalities in the short term due to the recent time that this architecture has in technological terms.

Key words: Architecture, comunnications, model, management, protocols, SDN,

Introducción

A nivel empresarial las redes internas de comunicaciones tienden a ser complejas por la cantidad de servicios solicitados por los usuarios, las empresas siguen creando productos y servicios basados en redes comerciales, a menudo mediante el uso de tecnologías nuevas y no convencionales (Comer, 2015).

La Unión Internacional de Telecomunicaciones (UIT) como ente que rige las normalización y estandarización de las telecomunicaciones establece en la norma M.3400 las funciones de la red de gestión de telecomunicaciones dividiéndolas en 5 áreas funcionales como son: gestión de la calidad de funcionamiento (desempeño), gestión de averías (fallas), gestión de la configuración, gestión de la contabilidad y gestión de la seguridad (UIT, 2000). Este modelo se ha popularizado como el modelo FCAPS (por sus siglas en inglés) para caracterizar el alcance de la administración de redes (Comer, 2015: p.534) y que se considera genérico y de aplicación a cualquier tipo de red.

Las redes definidas por software (SDN, por sus siglas en inglés) son un paradigma que comienza su primeros desarrollo en los años 90 con la introducción de funciones programables en la red, su segunda etapa se da entre el 2001 y 2007 con el desarrollo de interfaces abiertas en los planos de control y de datos, su tercera etapa con el desarrollo de OpenFlow y los sistemas operativos de red en el período del 2007 al 2010 (Feamster, Rexford y Zegura, 2014: p. 88) para finalmente desarrollarse por parte de la IETF en los años 2014 y 2015 las recomendaciones RFC 7149 y RFC 7426 respectivamente, donde se detallan las perspectivas de SDN desde un operador de red, capas y terminología de la arquitectura.

SDN traslada las funciones de gestión desde el plano de control de un elemento de red hacia un controlador asociado, el cual no incluye una interfaz humana, sino que por medio de comandos de bajo nivel traslada los comandos al plano de datos o físico del equipo (Comer, 2015: p. 550). Esta separación de los planos de control y de datos permite realizar ajustes a la configuración de los elementos de red, atención de averías, recolección de indicadores de desempeño de una manera dinámica. Los elementos de red se agrupan en clusters y el controlador gestiona un cluster.

Entonces, la implementación de la arquitectura SDN en principio plantea dos escenarios, al parecer distintos en términos de gestión de redes de telecomunicaciones. El primero es el escenario propuesto por FCAPS, en donde utilizando el protocolo de gestión simple (SNMP), bajo un modelo agente – gestor no hay separación de capas o modelo tradicional. El segundo es el incorporado por SDN, que es un modelo distribuido y dinámico, donde un controlador se encarga de las funciones de gestión sobre los elementos, separando los planos de control y físico de estos. Es así, como este estudio descriptivo plantea que ambos escenarios pueden converger, y tomando esto como punto de partida, realizar un análisis de la gestión de SDN desde la perspectiva de FCAPS.

Fundamento teórico

Modelo FCAPS: El modelo FCAPS es desarrollado por la UIT en la norma M.3400 del año 2000. El modelo pretende estandarizar en 5 funciones la administración de las redes, esto bajo un esquema genérico para que su aplicación no sea dependiente de una tecnología o medio específico (UIT, 2000: p. 2).
El modelo FCAPS establece las siguientes áreas:

•Gestión de calidad de funcionamiento o de desempeño: Proporciona funciones destinadas a evaluar el comportamiento de equipos de telecomunicaciones e informar al respecto. El objetivo es reunir y analizar datos estadísticos para supervisar y corregir el comportamiento y la efectividad de la red, del elemento de red o del equipo de red, para así facilitar la planificación, provisión, mantenimiento y medición de la calidad. (UIT, 2000: p. 6).

•Gestión de fallas o gestión de averías: Permite a un administrador localizar eventos que están provocando

la interrupción del servicio o degradación en el nivel de servicio acordado y recuperar la operación normal en el menor tiempo posible. Las posibles fallas incluyen software, enlaces, equipos (Comer, 2015: p. 535).
•Gestión de Configuración: Permite conocer el funcionamiento de una red desde la perspectiva de conexión física y lógica de sus equipos, desde su construcción hasta su implementación. Es en la función donde se puede obtener la información para determinar si el estado del elementos y de la red es de operación normal o se encuentra en estado de falla.

•Gestión de la contabilidad y facturación: Esta gestión corresponde más a una empresa operadora y proveedor de servicios de telecomunicaciones comerciales, porque en las redes empresariales, no se realiza una facturación por el uso o tráfico dentro de las redes de comunicación, sino que se carga a una contabilidad de costo, similar al costo de consumo eléctrico o de agua potable. Pero en los proveedores de servicios de internet (ISP, por sus siglas en inglés) es un aspecto crítico (UIT, 2000: pp. 61-69).

•Gestión de la seguridad: Comprende los servicios de seguridad de las comunicaciones, la detección y notificación de eventos de seguridad (UIT,2000: p. 70). Es uno de los aspectos más complejos dentro del modelo FCAPS, puesto que es transversal a una serie de protocolos y dispositivos, donde su modelo debe buscar al eslabón más débil y a partir de ahí realizar la construcción del modelo (Comer, 2015: p.535).

Protocolo SNMP: El protocolo de gestión de red simple (SNMP, por sus siglas en inglés) es el protocolo estándar para la gestión de redes. Este permite definir con exactitud la forma en que un administrador se comunica con el agente del gestor, para lo cual se define un formato de solicitud desde el administrador al agente y un formato de respuesta desde el agente al administrador (Comer, 2015: p.539). Esto se define desde la versión 1 de SNMP, como menciona Oancea (2003: p 82) específicamente cuando se define la estructura de la gestión de información (SMI, por sus siglas en inglés), la cual establece las reglas para describir la información de gestión, por medio de la Notación de Sintaxis Abstracta (ASN.1, por sus siglas en inglés). Esto le permite a SNMP identificar los tipos de mensaje que pueden ser enviados de un administrador a un agente, los formatos de esos mensajes y los protocolos de comunicación que deben ser usados (Feit, 1993: pp. 31-32). En la figura 1, se ilustran los tipos de mensajes que son incluidos en la comunicación administrador – agente conforme a SNMP v1.

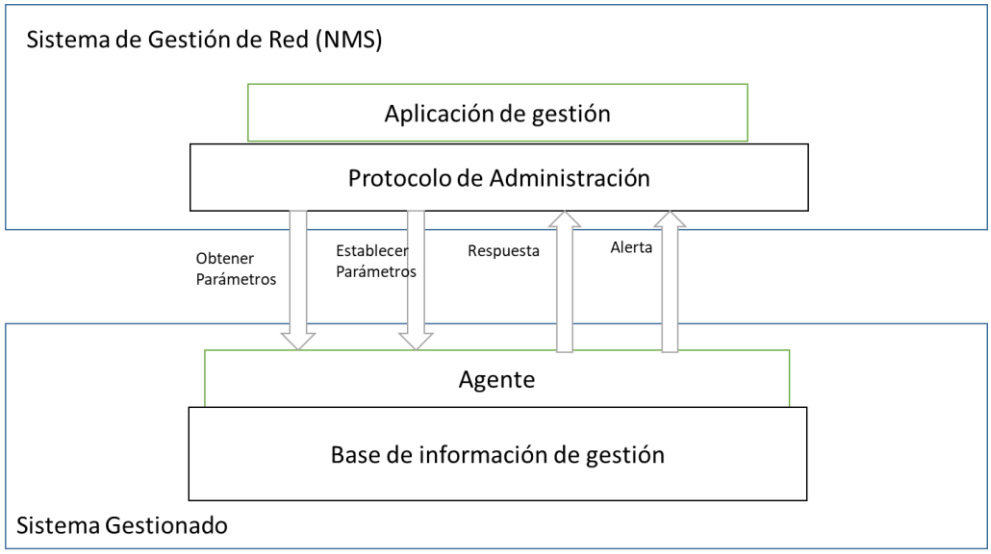

Figura 1. Tipos de mensajes en SNMP v1.

En la versión 2 se incluyeron dos tipos de mensajes adicionales de comunicación entre el agente y el gestor, además de modificar los mensajes de alertas (traps). En la versión 3, actualmente vigente, se incluyeron los modelos de seguridad basado en el usuario y control de acceso por vistas, con los cuales se protege el

acceso a la información de la base de información de gestión (MIB, por sus siglas en inglés) (Molero, 2010).

Redes SDN: El paradigma de SDN establece un controlador asociado a un mecanismo manejado por software, el cual asume la mayoría de las funciones del plano de control de un elemento de red, esto significa que desde una PC se podría reconfigurar toda la red con protocolos de bajo nivel (capa 1 a 3 del modelo OSI), cuando este controlador determine que así lo requiera por algún parámetro preestablecido y se comunique directamente con el plano de datos (Comer, 2015: p. 550). Como se visualiza en la figura 2.

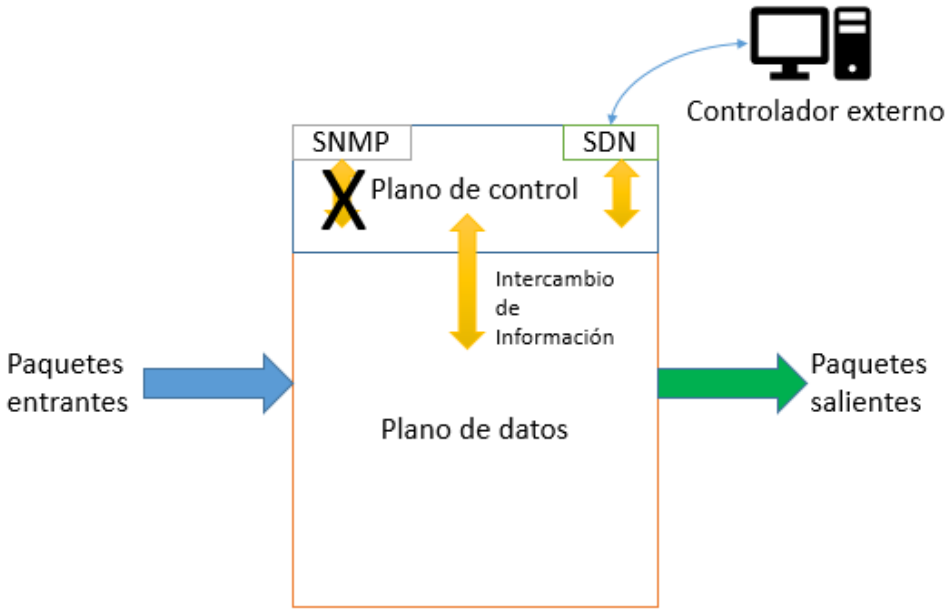

Figura 2. Controlador externo de SDN

Un elemento de red se dimensiona en dos planos: el plano de datos (físico) y el plano de control (lógico). Estos dos planos interactúan a través de un agente instalado en el plano de control, de tal manera que la red de gestión pueda obtener datos y parámetros sobre el funcionamiento del elemento de red al utilizar protocolos como SNMP. Aun cuando, el protocolo es un estándar, la IETF a través de las RFC, permite libertad a los diseñadores de reescribir o incorporar funcionalidades según lo requieran (Feit, 1993: p. 577). Esto origina que los desarrolladores de equipos de red incorporen una interfaz estándar de administración para la comunicación hacia la red de gestión. Inclusive protocolos "propietarios" que no permiten la interoperabilidad, y de ahí que se requieran gestores propios o en su defecto, desarrollos adicionales en las redes de gestión (Comer, 2015: p. 549) para facilitar la interoperabilidad entre protocolos de gestión.

El paradigma SDN genera una incertidumbre en los administradores de red, porque el incluir un controlador externo para cada elemento de red conlleva a una solución costosa a nivel de equipamiento. Los diseñadores de SDN establecen que un solo controlador puede controlar varios elementos, considerando que un protocolo de administración no actúa constantemente sobre los elementos de red, sino cuando es requerido. Con eso crean y conceptualizan los dominios de SDN, de tal manera que cada controlador administra un dominio, como se muestra en la figura 3.

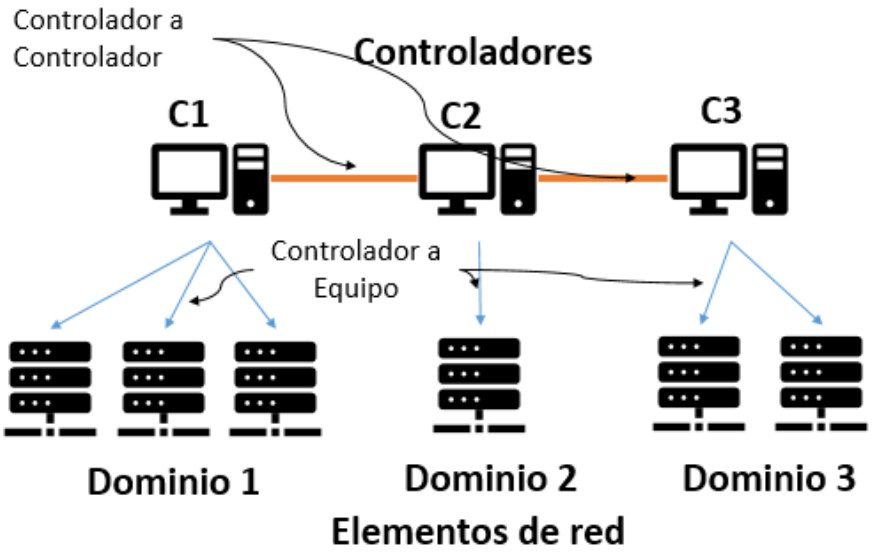

Figura 3. Dominios SDN.

Open Flow: Open Flow es el protocolo de comunicación que define el contenido y el formato de mensaje que se intercambian entre el plano de datos y el plano de control, con la adopción de este protocolo SDN logra operar en redes que tienen elementos de red de diferentes proveedores (Apostolidis, 2015: p. 15). OpenFlow especifica paradigma de la comunicación, definición y clasificación de elementos y formato de los mensajes (Comer, 2015: p. 554). A diferencia de SNMP el protocolo OpenFlow es orientado a conexión, por lo que su protocolo de transporte es TCP y no UDP. Además, OpenFlow usa como mecanismo de seguridad SSL, por lo cual establece una conexión segura entre el controlador y el elemento. Eso significa que los controladores deben abrir una sesión TCP por cada elemento que se administra.

El controlador tiene el rol de sistema operativo (OS, por sus siglas en inglés) para la red e implementa el plano de control de ésta. También, el controlador implementa las políticas de red y controla los dispositivos SDN que pertenecen a la red y proporciona la interfaz hacia las API de usuario. Y a bajo nivel, su interfaz permite la comunicación con los conmutadores OpenFlow. En la figura 4 se describen los principales componentes que tiene el controlador OpenFlow.

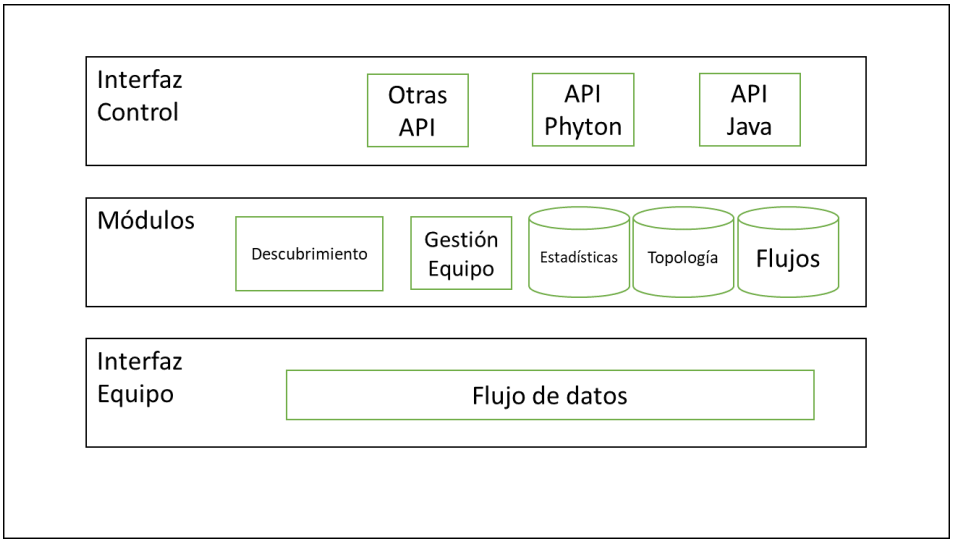

Figura 4. Componentes del controlador OpenFlow

Metodología

El diseño metodológico de este trabajo es de teoría fundamentada. Como indica Hernández, Fernández y Baptista (2010) se utiliza un procedimiento sistemático cualitativo para generar una teoría que explique una situación o contexto particular (pp. 492 – 493). En este caso, se construye una teoría a partir de la revisión bibliográfica de la aplicación del modelo FCAPS en redes SDN.

El procedimiento tiene como primera fase una revisión bibliográfica de la revisión de normativa de la ITU-T de la serie M.3400 en donde se detalla el modelo FCAPS y de esta manera obtener las funcionalidades por analizar. También, se realiza una revisión de los RFC de la IETF relacionados al desarrollo de SDN y OpenFlow, con esto obtener las funcionalidades de este protocolo.

De esta manera, se tienen los fundamentos normativos relacionados a ambos elementos en estudio: FCAPS y la arquitectura SDN. En el siguiente paso, mediante el uso motores de búsqueda en internet como Google académico, bases de datos de CONARE y bases de universidad internacionales, así como repositorios de congresos, seminarios, como son IEEExplorer, Researchgate, ScienceDirect y con la aplicación de sintaxis de búsqueda y operadores lógicos como AND, OR dependiendo de lo solicitado por el repositorio se ubican trabajos en el ámbito académico y profesional.

Los términos buscados fueron: management, SDN, FCAPS, architecture, OpenFlow, comparative, protocol, OpenFlow y combinaciones de estos. Los términos se usaron en inglés por cuanto el mayor porcentaje de bibliografía se encuentra en dicho idioma. Además, se incorporaron filtros en términos de períodos de estudio primeramente del año 2016 a la fecha, posterior se aumentó del 2010 a la fecha. En el caso de las normativas, se utilizaron las últimas versiones aprobadas, aun cuando como en el caso de las ITU corresponde a períodos de hasta hace 20 años, pero son las vigentes.

Con las fuentes identificadas se procedió al tercer paso: selección, clasificación y priorización. Para seleccionar las fuentes se establecieron filtros como períodos de tiempo, de manera similar a los filtros usados en los motores y repositorios. Además, se usaron parámetros asociados a las temáticas de estudio: telecomunicaciones, gestión, redes con lo cual tener un segundo nivel de selección. En un tercer nivel dentro del proceso de selección se procedió a la lectura del resumen, palabras claves y metodologías del documento con esto se finaliza el proceso de descarte de fuentes.

Para la categorización de las fuentes se hizo de una plantilla de ficha bibliográfica en donde se pudo categorizar las fuentes por temáticas, contenidos, fechas, entre otros parámetros. Además, la ficha contenía una sección de resumen de la fuente, en donde se sistematizo la información de cada fuente: objetivos, métodos, resultados y conclusiones.

Una vez categorizadas las fuentes se procedió a priorizarlas. Para realizar esta acción, se dio lectura a cada fuente y revisó cada ficha de la fuente, estableciendo una relación primaria o complementaria al tema de la investigación. En el caso de las normativas, estas se contemplan como de carácter obligatorio de cara al ente normalizador, por lo cual su validación es por su carácter de cumplimiento.

En la cuarto etapa del trabajo, se realiza la redacción de la investigación. En esta etapa se construyeron resúmenes de cada fuente, se integraron datos y resultados, con lo cual poder fundamentar y establecer la teoría de aplicación de FCAPS sobre SDN, de una manera descriptiva. Primero se estudió la normativa M.3400 de la ITU-T de donde se comprenden las funcionalidades del modelo FCAPS. En segundo lugar, de las fuentes relacionadas a OpenFlow y SDN se establecen las características y modalidades de gestión en esta arquitectura. En el tercer paso de esta etapa se realizó un emparejamiento de similitudes y diferencias entre lo propuesto para SDN y los indicado en el modelo FCAPS. De esta manera se llega a la redacción de los resultados y valoraciones sobre la posible aplicación de FCAPS sobre SND.

Discusión y resultados

Administración de SDN desde la perspectiva de FCAPS

Bajo el modelo FCAPS, el controlador de SDN se puede considerar un gestor. Este componente asume funciones de configuración, de atención de fallas y evaluación de rendimiento, de manera similar al gestor en FCAPS. Si es claro que el controlador no puede asumir todas las funciones asignadas a un gestor FCAPS, pero al menos en su cluster de elementos de red, permite la realización de funciones primarias de gestión.

En el modelo FCAPS el gestor existe por practicidad. El modelo de gestión de red sobre el cual actúa FCAPS es centralizado, entonces de manera práctica un gestor asume todas las funciones dando mayor control son las funciones, así como de los cambios que esto provoca. Un modelo estandarizado y probado desde su concepción en la década de los años 90 del siglo XX.

En el caso del controlador SDN la propuesta es recargar en el controlador ambos roles (gestor y controlador), lo cual abre la posibilidad de un fallo o incidente. Por eso, a nivel de SDN es fundamental establecer cuáles y cuántas serán las funciones de administración que puede asumir el controlador (Abdallah, 2018: p.2). Por eso, el análisis del protocolo OpenFlow desde el contexto FCAPS provee información para establecer si es capaz de soportar la gestión de SDN, si se requiere de protocolos complementarios para lograr una gestión efectiva en SDN o si el software de gestión de red puede consultar la información FCAPS en redes SDN (Apostolidis, 2015: p. 23).

Los resultados de los análisis realizados se presentan por cada una de las gestiones que componen FCAPS.

Gestión de Fallas: Desde la perspectiva de gestión de fallas o averías, un aspecto medular en la gestión es el tiempo de recuperación de la red a su operación normal. Cada red es distinta, por ejemplo, Nived-Jenkins et al (2009), establecen el valor en 50 ms en enlaces MPLS con redundancia como un valor aceptable. Para SDN se tienen dos modelos de control, el primero llamado In-band donde el canal de control entre el controlador y el equipo comparte la interfaz física de comunicación con el enlace de datos. En el segundo modelo, llamado out-band los canales de datos y de control se separan físicamente. Tal y como se muestra en la figura 5.

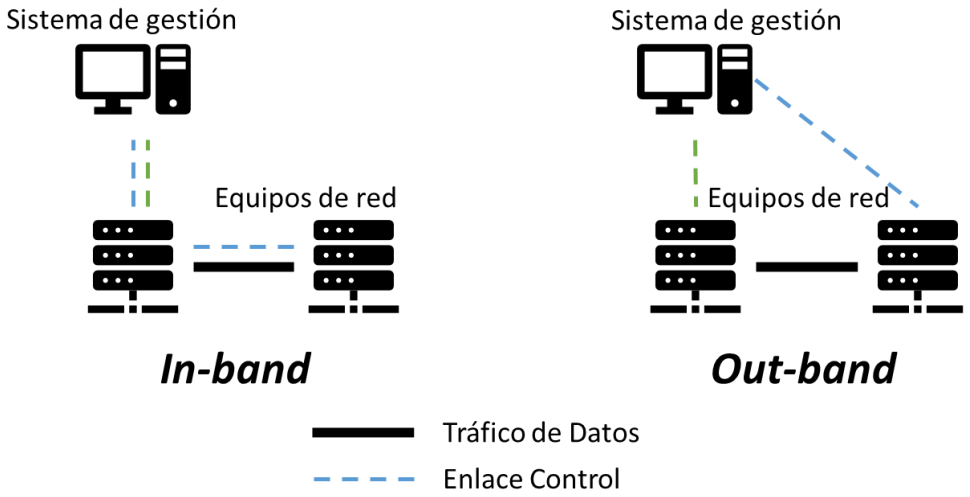

Figura 5. Esquema de la conexión In-band y Out-band de SDN

Además, en SDN se establecen mecanismos para recuperación y mecanismos de protección. Los primeros son orientados a la atención reactiva del evento, como una caída en el enlace de comunicación, o sea, se presenta un cambio en el port-status. Y los segundos, son orientados a configuraciones que permitan prever el evento y generar una serie de acciones que están preconfiguradas para mantener la comunicación y generar un restablecimiento.

Entonces, en el caso de SDN, experimentos como el de Sharma et al (2013) demuestran que solo los esquemas de protección logran los 50 ms en redes complejas, y los mecanismos de recuperación solo obtienen los 50 ms en redes pequeñas. En el 2016, Sharma et al le dan seguimiento al trabajo, y llegan a las mismas conclusiones, bajo la exploración de los dos esquemas: protección y recuperación (p. 111). Aunque OpenFlow permite flexibilidad en la programación de las redes sin depender de un protocolo de distribución, el tiempo que toma para que un controlador responda y reconfigure los reenvíos de datos no facilita la respuesta de recuperación (Capone et all, 2015).

Varios mecanismos se han propuesto, como el uso de un protocolo de descubrimiento en la capa de enlace (LLDP), pero este protocolo tiene limitaciones de escalabilidad por el volumen de mensajes que llegan al controlador y requieren de recursos de procesamiento (Kempf et al, 2012) .Otro aspecto, del cual todavía SDN no se ocupa, es el tema de los datos provenientes de los elementos (tanto de comunicación como de soporte), que se han denominado non-flow data. Estos datos no aportan información inmediata sobre el rendimiento de los flujos de comunicación, sino sobre el estado de salud de un submódulo como pueden ser fuentes de alimentación, ventiladores. En este caso, se utilizan mecanismos existentes para el monitoreo de salud del dispositivo como SNMP, que podría adaptarse al enfoque de SDN en esta parte.

Gestión de Configuración: En el enfoque tradicional, en temas de configuración, el gestor lo que mantiene es una base de información con la configuración y parámetros del equipo, pero este tiene una independencia por medio de un sistema operativo que reside en cada elemento de red para configurar sus rutas y reenvíos de datos. Entonces, la operación de una red se fundamenta en un modelo distribuido y con autonomía por cada equipo (Apostolidis, 2015: pp. 28-29).

En el caso de SDN, establece que un sistema operativo de red centralizado puede asumir ciertas funciones que son admitidas dentro de la gestión de configuración, entre estas las que tienen que ver con: mantener la topología de red, gestión de los cambios en la topología y estado de la red, transferir los cambios en la red a los aplicativos y equipos (Devlic, 2012).

Pero SDN no puede asumir algunas funciones de configuración como asignar una dirección IP a un equipo de red. Entonces, para esto se desarrolló un protocolo complementario denominado OF-Config, que mediante un punto de configuración se logra la comunicación entre el controlador mediante los mensajes de OF-Config a un switch. De esta manera se proporcionan algunas funcionalidades de configuración como: asignación de direcciones IP, configuración de la capa de transporte usada en las comunicaciones, configuración de umbrales y puertos, habilitación o des habilitación de puertos, ajuste de velocidad en los puertos. Aun así, en ciertas funciones como la de configuración de la red física, se requiere del uso de otros protocolos tradicionales como LLDP, para la obtención de información como topología física que descubre el elemento de red. Estudios como el de Devlic et all (2012), han demostrado que OF-Config puede asumir las funcionalidades de configuración, sin embargo, sus limitaciones no vienen de la aplicación, sino de los sistemas legados a los cuales se debe conectar SDN, porque estos no soportan al protocolo, por lo cual no reciben instrucciones de éste ni tampoco permitirían llenar la base de datos de configuración.

Gestión de Contabilidad: La gestión de la contabilidad, desde la perspectiva de FCAPS se ha relacionado con los cargos para el usuario en operadores de red o el uso de los recursos de red en redes corporativas. La funcionalidad se ve desde la perspectiva de obtener estadísticas del uso de los recursos a nivel de la red, e identificar individualmente el uso de los recursos por parte del usuario.

Para que SDN cumpla con este aspecto, debe identificar tanto al usuario como al recurso del cual está haciendo uso, y a través de aplicación de capa superior, enviar la información para la generación de reportes, transacciones y hasta para facturación entre departamentos (Apostolidis, 2015: p. 34). En la

especificación de OpenFlow 1.5.0 se establecen campos para la identificación de estos elementos, como por ejemplo fuente IP, puerto de ingreso, puerto de salida, destino IP. Y mediante una asociación de direcciones IP con los usuarios, se puede lograr la identificación deseada. Dentro de los posibles contadores que se puede obtener con OpenFlow se encuentran paquetes recibidos, paquetes enviados, bytes transmitidos, bytes recibidos, errores recibidos, tiempo de la conexión, entre otros.

Aunque, los controladores OpenFlow pueden conocer las estadísticas de los equipos, se debe realizar la gestión de los usuarios de red, que está relacionada directamente con el tema de la contabilidad. Por lo cual, los usuarios de la red deben ser reconocidos en un flujo de SDN, lo cual es casi imposible de mapear en los ingresos a un switch, para esto se debe hacer uso de la autenticación del usuario para correlacionar su id, dirección IP y flujos de entrada. Al igual que en los casos anteriores, OpenFlow por sí solo no puede realizar estas funciones. Es así, como la RFC 3176 InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks (Phaal, 2001) establece que se puede usar los motores sFlow-RT para asociar las estadísticas en tiempo real de los usuarios.

Gestión del Desempeño: El dilema de la gestión de desempeño o rendimiento parte de los modelos existentes para su ejecución. El modelo pasivo permite sin agregar tráfico a la red obtener datos que permitan analizar y medir el desempeño de la red, esto no genera encabezados adicionales, pero si requiere de la instalación de ciertos puntos de monitoreo y, además, no se puede implementar en cualquier red de comunicación. En el caso, del método activo, éste agrega tráfico a la red que es exclusivo para las mediciones, no agrega infraestructura adicional, pero si puede ocasionar un desmejoramiento a los indicadores globales de la red, por esa inclusión de tráfico. Por ejemplo, ICMP puede utilizarse para medir el retardo en una comunicación, pero a su vez carga de solicitudes echo a la red de datos.

El trabajo de van Adrichem et all (2014) demostró que OpenNetMon permite a SDN monitorear indicadores como pérdida de paquetes, retardos de envío en paquetes, entre otros, aprovechando las características de OpenFlow. El método usado por OpenNetMon para recuperar las estadísticas es el envío de un flujo de bytes y la duración de éste, con eso se calcula la efectividad por cada flujo (pp. 3-4). Uno de los puntos abordados por OpenNetMon y de los principales a nivel de desempeño o rendimiento, es el tema de mantener el monitoreo sin afectar el rendimiento del enlace a través del cual se presta el servicio al usuario y sin generar costos adicionales. Por ejemplo, un servicio de vídeo de alta definición puede variar su velocidad desde 1 Mbps hasta 9 Mbps o más, entonces para mantener el monitoreo OpenNetMon, adapta su muestreo al perfil que tiene el tráfico. En algunos puntos de lo documentado por van Adrichmen et all, no siempre se logra la sincronización del muestreo con el tráfico de la red, asumiendo los autores que es la no sincronización de las configuraciones es la causa de estas imprecisiones.

Otro aspecto, que en SDN y desde OpenFlow se puede trabajar es la medición de los paquetes perdidos. Inicialmente, los diseñadores de SDN lo estimaron a partir de una relación lineal, entre lo enviado y lo perdido, pero ese comportamiento está demostrado que no es correcto. Por lo cual se desarrolla una técnica alternativa y aplicable, ésta es la recuperación de un flujo estadístico de paquetes entrantes y saliente por cada camino del conmutador. Entonces, la relación entre ambos permite una estimación más cercana del indicador. También es posible en SDN usar las estadísticas de flujo de OpenFlow como monitoreo de tráfico, esto por medio de la técnica OpenTM que realiza el seguimiento a estos flujos y permite la creación de una matriz de tráfico (TM) (Du, Q and Zhuang, H; 2015). Así el controlador SDN puede crear una TM consultando a los interruptores OpenFlow periódicamente en intervalos fijos, y el estudio arroja que son más precisos cuando el interruptor o sensor se encuentra al final de la ruta.

También se detallan trabajos como el de Minlan, Lavanya y Rui (2013) que proponen una alternativa denominada arquitectura OpenSketch en la cual se realiza una separación de las medidas de los planos de control y de datos, introduciendo una API con dicho objetivo. El problema de esta solución significa remplazar nodos de red existentes, y eso representa un costo muy alto para los operadores y redes corporativas.

Gestión de la seguridad: Open Flow permite el control de flujos específicos dentro de la gestión de red. Esto permitiría el marcar algunos flujos como hostiles si cumplen con ciertos criterios definidos en las políticas de seguridad. Parte de los procedimientos que se pueden establecer es el envío de este flujo hostil a direcciones específicas o métodos más complejos para eliminación y determinación del origen del flujo. Se pueden implementar políticas básicas basadas en listas de acceso (ACL) considerando las características de OpenFlow y con ellos revisar campos en los paquetes como dirección fuente, dirección destino, protocolo de transporte TCP/UDC. En el caso de técnicas más avanzadas requieren de un análisis de las acciones sobre los campos que no pueden ser emparejado por OpenFlow, esto es como las URL's, nombres de host, los cuales pueden venir en el paquete de datos y podrían no examinarse.

SDN también presenta otra limitante a nivel de seguridad, y es la falta de conocimiento de estado del flujo (Apostolidis, 2015: p. 45). En la última versión de SDN no se específica algún aspecto sobre la conducta de los flujos de información, por lo cual se deben usar elementos especializados, tanto físico como lógico para lograr esta funcionalidad de la seguridad. Esto por cuanto, OpenFlow lo que revisa es el encabezado del paquete, como se observa en la figura 6.

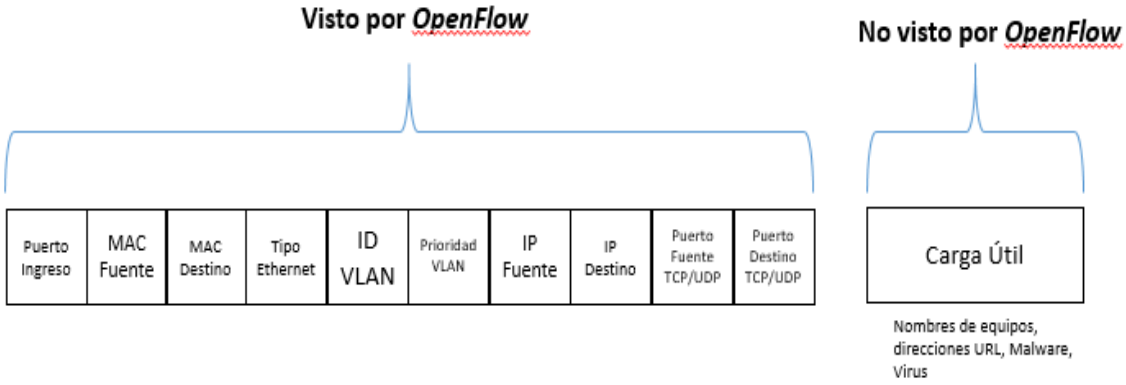

Figura 6. Revisión del encabezado por parte de OpenFlow

El estudio de Porras et all (2015) muestra que, si bien OpenFlow no tiene los mecanismos completos para cumplir con todas las funcionalidades de seguridad conforme al modelo de FCAPS, se establece que con cuatro algoritmos en detección de amenazas junto con el controlador NOX se puede cumplir con algunas de estas. Estos mecanismos definidos son:

•TRW-CB: el algoritmo establece que un mensaje benigno establece más conexiones que uno malicioso.
•Limitación de envío: Establece que cuando un virus quiere propagarse, trata de establecer la mayor cantidad de conexiones en un tiempo mínimo.
•Detección de entropía máxima: Proporciona una distribución normal del tráfico, esto se debe estar revisando constantemente porque requiere de una examinación de cada paquete.
•NETAD: Este asume que una anomalía en el tráfico puede ser detectado con el primer paquete de conexión. Con lo cual, desde que se detecta la primera anomalía se rechaza todo paquete.

Uno de los mayores retos de la seguridad en SDN son los ataques de denegación de servicios (DDoS). Esto lo explica Apostodolis (2015) que se realiza mediante el monitoreo de los conmutadores OpenFlow durante intervalos definidos por el controlador NOX. Esto lo hace por medio de un módulo de clasificación, que desde el flujo entrante extrae aquellos que resultan interesantes. Este método propone entonces tres módulos: el colector de flujo, el extractor de las características y el clasificador, con esto se determina el ataque. Esto se ilustra en la figura 6.

Un aspecto que introduce SND diferente con respecto a las redes tradicionales es el punto central de control de la red. Este punto debe ser protegido contra los ataques, recordando el concepto básico de SND, al separar el plano de control y de datos, e introducir un controlador que centraliza el control completo de una red y su flujo de datos, entonces este punto se vuelve sensible a los ataques. La diferencia, es que en una red tradicional pueden ser miles de nodos, pero en redes SDN de similar tamaño la cantidad de controladores puede disminuir a unas decenas. Entonces, el tener centralizado el control introduce una serie de beneficios, pero también introduce una nueva modalidad de amenaza y posible tipo de ataque. Algunas de estas vulnerabilidades son: flujos de datos falsos, vulnerabilidades en los conmutadores OpenFlow, comunicaciones del plano de control comprometidas, vulnerabilidades en controladores, confianza entre las aplicaciones de gestión y controladores, entre otros.

Conclusiones

SDN no nace con la perspectiva de una gestión desde la visión de las normas ITU-T, pero del estudio realizado y revisión de distintas fuentes, se comprueba como el análisis de la gestión de red en SDN parte de la perspectiva de las funcionalidades que brinda FCAPS.

Con lo anterior, FCAPS mantiene el estatus de ser el modelo normalizado y estandarizado de aplicación en la gestión de red, que además es genérico y, por lo tanto, permite un análisis desde su perspectiva de otros tipos de gestiones.

En el caso de SDN, el estudio denota una serie de carencias desde la perspectiva de FCAPS pero que distintos desarrollos, los cuales aprovechan la flexibilidad del protocolo OpenFlow, han tratado de solventar. Al considerar el tiempo de desarrollo que tiene SDN es de esperar que pueda abarcar todas las funcionalidades, y esto reemplazaría el uso de protocolos de gestión tradicionales, como SNMP, en el marco de la gestión de red.

Los aspectos donde mayor atención deben poner los desarrolladores de OpenFlow es en fallas y seguridad, porque el tema de fallas y su recuperación, es de suma importancia para que los operadores adopten el esquema SDN como su estándar de red. En el tema de seguridad, un nuevo esquema introduce una serie nueva de vulnerabilidades que deben ser atendidas.

Agradecimientos

Se agradece el espacio brindado por el programa de Ingeniería de Telecomunicaciones para la realización de este artículo en paralelo a la elaboración de la unidad didáctica de la asignatura 03395. Si bien no hay uso de recursos ni financiamiento de por medio, al asignarse la labor de la unidad didáctica surgen una variedad de temas complementarios que permiten su desarrollo como complemento a la materia que se incorporará a la asignatura.

Referencias

Abdallah, S; Elhajj, I. H; Chehab, A and Kayssi, A. (2018). A Network Management Framework for SDN. *Proceedings of 9th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1-4) Paris, Francia: NTMS

Apostolidis, P. 2015. *Network management aspects in SDN* (tesis inédita para optar por el grado de Master of Science (MSc) in Information and Communication Systems, School of Science / Technology). International Hellenic University, Grecia. Recuperada de: https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/12435/Network%20management%20aspects%20in%20SDN.pdf?sequence=1.

Capone, A. Cascone, C. Nguyen, A. Sanso, B. (2015). Detour Planning for Fast and Reliable Failure Recovery in SDN with OpenState. Recuperado de: https://arxiv.org/pdf/1411.7711.pdf

Comer, Douglas E. (2015). *Redes de computadoras e internet*. México: Pearson Educación.

Devlic, A; John, W; Sköldström, P. (2012). A Use-Case Based Analysis of Network Management Functions in the ONF SDN Model. *Conferencia Software Defined Networking*. Recuperado de: https://www.researchgate.net/publication/261075940_A_Use-Case_Based_Analysis_of_Network_Management_Functions_in_the_ONF_SDN_Model

Du, Q; Zhuang, H. (2015). OpenFlow-Based Dynamic Server Cluster Load Balancing with Measurement Support. *Journal of Communications*, *10*(8): 572 – 578. Doi:10.12720/jcm.10.8.572-578

Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: an intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, *44*(2), 87-98.

Feit, Sidnie. (1993). SNMP: *A guide to network management*. Estados Unidos de América: McGraw-Hill.

Hernández, R., Fernández, C. y Baptista, P. (2010). Metodología de la investigación (5ª ed.). México: McGraw Hill.

Kempf, James & Bellagamba, Elisa & Kern, Andras & Jocha, David & Takacs, Attila & Sköldström, Pontus. (2012). *Scalable fault management for OpenFlow*. Recuperado de: https://www.researchgate.net/publication/261115864_Scalable_fault_management_for_OpenFlow

Minlan, Y; Lavanya, J; Rui, M. (2013). Software Defined Traffic Measurement with OpenSketch. *Proceedings of 10th Symposium on Networked Systems Design and Implementation* (pp.29–42), Illinois, Estados Unidos de América: NSDI'13. Recuperado de: http://stanford.edu/~lavanyaj/papers/opensketch12.pdf.

Molero, Luis. 2010. *Unidad II: Evolución del protocolo de gestión de internet*. Universidad Dr. Rafael Belloso Chacín. Recuperado de: https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-II.pdf

Niven-Jenkins, B; Brungard, D; Betts, M. (2009). *RFC 5654: Requirements of an MPLS Transport Profile*. Internet Engineering Task Force. Recuperado de: https://tools.ietf.org/html/rfc5654

Porras, P; Cheung, S; Fong, M; Skinner, K; Yegneswaran, V. (2015). *Securing the Software-Defined Network Control Layer*. Recuperado de: http://www.csl.sri.com/users/vinod/papers/sefloodlight.pdf.

Phaal, P; Panchen, S; McKee, N. 2001. *RFC 3176: InMon Corporation's sFlow: A method for monitoring traffic in switched and routed networks*. Internet Engineering Task Force. Recuperado de: https://www.ietf.org/rfc/rfc3176.txt.

Oancea, Daniel. 2003. Structure of Management Information in SNMP. *The Annals of "DUNAREA DE JOS"*. *3*: 82-85.

Sharma, S; Staessens, D; Colle, D; Pickavet, M and Demeester, P. (2013). OpenFlow: Meeting carrier-grade recovery requirements. *Computer Communications. 36*: 656–665. Recuperado de: https://www.researchgate.net/publication/256942138_OpenFlow_Meeting_carrier-grade_recovery_requirements

Sharma, S., Staessens, D., Colle, D., Pickavet, M., & Demeester, P. (2016). In-band control, queuing, and failure recovery functionalities for OpenFlow. IEEE NETWORK, 30(1), 106-112. Recuperado: https://biblio.ugent.be/publication/7105700/file/7105706

Unión Internacional de Telecomunicaciones. (2000). *Funciones de gestión de la red de gestión de telecomunicaciones*. Recuperado de: https://www.itu.int/rec/T-REC-M.3400/es

Van Adrichem, NLM., Doerr, C., & Kuipers, FA. (2014). OpenNetMon: network monitoring in openflow software-defined networks. In J. Janusz Filipiak (Ed.), *Proceedings NOMS* (pp. 1-8). Piscataway: IEEE Society. https://doi.org/10.1109/NOMS.2014.6838228

.